

Title: Machine tool protected against improper activation and method of avoiding improper machine activation by machine control parameters for this

Patent claims

1. Machine tool (2, 2a) protected against improper activation, which has

an open-loop and/or closed-loop control device for the activation of machine functions, preferably machine axes (σ_1 , σ_2), and

means for reading in machine control parameters for the open-loop and/or closed-loop control device from a data carrier or electronic carrier signal (3),

characterized in that it has an improper-activation safety module, preferably an improper-activation safety software module, which decodes the machine control parameters again that are intended for the machine tool and are encoded by means of an asymmetric encryption method, using an encryption key which is assigned to the machine tool (2, 2a) and provided for the encryption, with the aid of a decryption key which is likewise assigned to the machine tool (2, 2a), is different from the encryption key and is provided for the decryption, and which module enables the machine control parameters for controlling the machine tool (2, 2a) only in the case of successful decryption.

2. Machine tool (2, 2a) protected against improper activation according to Claim 1, characterized in that the machine tool has a reading module, preferably a chip card reader, which is intended for receiving a decryption module, preferably a

chip card, which has the decryption key, with the aid of which the improper-activation safety module decodes the encoded machine control parameters, and the decryption module is set up in such a way that only the improper-activation safety module can read out the decryption key from the module.

3. Machine tool (2, 2a) protected against improper activation according to Claim 1 or 2, characterized in that the improper-activation safety module determines the successful decryption of the machine control parameters after the decryption on the basis of finding a machine identification assigned to the machine tool (2, 2a).
4. Machine tool (2, 2a) protected against improper activation according to Claim 1, 2 or 3, characterized in that the improper-activation safety module enables various functions of the machine tool (2, 2a) for control by the machine control parameters in dependence on the decryption key originating from a plurality of decryption keys assigned to the machine tool (2, 2a).
5. Machine tool (2, 2a) protected against improper activation according to one of Claims 1 to 4, characterized in that the improper-activation safety module determines the successful decryption of the machine control parameters after decryption also on the basis of finding a signature of a unit authorized for activating the machine tool (2, 2a).
6. Machine tool (2, 2a) protected against improper activation according to Claim 5, characterized in that the improper-activation safety module enables various functions of the machine tool (2, 2a) for control by the machine control parameters in dependence on which signature it finds after decryption from a plurality of signatures.

7. Method of avoiding improper machine activation by machine control parameters of a machine tool (2, 2a), characterized in that the machine control parameters intended for the machine tool are encoded by means of an asymmetric encryption method with the aid of an encryption key which is assigned to the machine tool and is provided for the encryption, so that the machine tool can decode the machine control parameters again with the aid of a decryption key which is likewise assigned to it, is different from the encryption key and is provided for the decryption.
8. Method of avoiding improper machine activation by machine control parameters of a machine tool (2, 2a) according to Claim 7, characterized in that a machine identification assigned to the machine is added to the machine control parameters before the encryption, so that, when it decodes the machine control parameters again with the aid of its assigned private decryption key, the machine tool can determine on the basis of the fact that these contain the machine identification assigned to it that the parameters concerned are machine control data for its activation.
9. Method of avoiding improper machine activation by machine control parameters of a machine tool (2, 2a) according to Claim 7 or 8, characterized in that the machine control parameters intended for the machine tool are first encoded by means of a private decryption key, assigned to the sender of the machine control parameters, and are provided with a sender identification of this sender, and, signed by the sender in this way, are only encoded with the aid of the encryption key that is assigned to the machine tool and known for the encryption.

10. Computer system (1) with at least one data processing unit and at least one memory, characterized in that the data processing unit is set up in programming terms in such a way that it works on the basis of the method according to one of Claims 7 to 9.
11. Computer program which has instructions which are set up for carrying out the method according to one of Claims 7 to 9.
12. Computer program product which has a computer-readable medium with computer program coding means, with which, after loading the computer program, a computer is made by the program to carry out the method according to one of Claims 7 to 9.
13. Computer program product which has a computer program on an electronic carrier signal, with which, after loading the computer program, a computer is made by the program to carry out the method according to one of Claims 7 to 9.
14. Data carrier or electronic carrier signal (3) with machine control parameters for reading into a machine tool (2, 2a) according to one of Claims 1 to 6, characterized in that

on the data carrier or the electronic carrier signal there are machine control parameters for the machine tool (2, 2a) which are encoded by means of an asymmetric encryption method with the aid of an encryption key which is assigned to the machine tool and is provided for the encryption, so that the machine tool can decode them again with the aid of a decryption key which is likewise assigned to it, is different from the encryption key and is provided for the decryption, and

the data carrier or the electronic carrier signal (3) controls the machine tool (2, 2a) by means of these machine control parameters during reading-in or after reading-in after they have been decoded.

15. Data carrier or electronic carrier signal (3) with machine control parameters according to Claim 14 for reading into a machine tool (2, 2a) according to one of Claims 1 to 6, characterized in that on the data carrier or the electronic carrier signal there is at least one machine identification included in the encryption and assigned to the machine tool (2, 2a), so that, when it decodes the machine control parameters again with the aid of its assigned private decryption key, the machine tool can determine on the basis of the fact that these contain the machine identification assigned to it that the parameters concerned are machine control data for its activation.
16. Data carrier or electronic carrier signal (3) with machine control parameters according to Claim 14 or 15 for reading into a machine tool (2, 2a) according to one of Claims 1 to 6, characterized in that on the data carrier or the electronic carrier signal there are machine control parameters for the machine tool (2, 2a) which are first encoded by means of a private encryption key, assigned to the sender of the machine control parameters, and are provided with a sender identification of this sender, and, signed in this way, are only encoded with the aid of the encryption key that is assigned to the machine tool and known for the encryption.
17. A method of generating machine control parameters for a machine tool (2, 2a) according to one of Claims 1 to 6, characterized in that

at least one data carrier or electronic carrier signal (3) with machine control parameters according to one of Claims 14 to 16 is generated.

18. Computer system (1) for generating machine control parameters for a machine tool (2, 2a) according to one of Claims 1 to 6 with at least one data processing unit and at least one memory, characterized in that the data processing unit is set up in programming terms in such a way that it generates at least one data carrier or an electronic carrier signal (3) with machine control parameters according to one of Claims 14 to 16.
19. Computer system (1) according to Claim 18 for generating machine control parameters for a machine tool (2, 2a) according to one of Claims 1 to 6, characterized in that the computer system (1) has a reader, preferably a chip card reader, which is intended for receiving an encryption module, preferably a chip card, which has the encryption key, with the aid of which the computer system encodes the machine control parameters, and furthermore an encoding module, preferably an encoding software module, is provided for encoding the machine control parameters, the encryption module being set up in such a way that only the encoding module can read out the encryption key from the module.
20. Computer program which has instructions which are set up for carrying out the method according to Claim 17.
21. Computer program product which has a computer-readable medium with computer program coding means, with which, after loading the computer program, a computer is made by the program to carry out the method according to Claim 17.

22. Computer program product which has a computer program on an electronic carrier signal, with which, after loading the computer program, a computer is made by the program to carry out the method according to Claim 17.

23. Computer control system for avoiding improper machine activation by machine control parameters for a machine tool (2, 2a) with

a computer system (1) according to Claim 18 or 19 for generating machine control parameters for a machine tool (2, 2a) according to one of Claims 1 to 6 or

a computer program according to Claim 20 or

a computer program product according to Claim 20 or 21,

and at least one machine tool (2, 2a) according to one of Claims 1 to 6.

Title: Machine tool protected against improper activation and method of avoiding improper machine activation by machine control parameters for this

Abstract

Machine tool (2, 2a) protected against improper activation, which has an open-loop and/or closed-loop control device for the activation of machine functions, preferably machine axes, and means for reading in machine control parameters for the open-loop and/or closed-loop control device from a data carrier or electronic carrier signal (3), and which has an improper-activation safety module, preferably an improper-activation safety software module, which decodes the machine control parameters that are intended for the machine tool and are encoded by means of an asymmetric encryption method, using an encryption key which is assigned to the machine tool (2, 2a) and provided for the encryption, with the aid of a decryption key which is likewise assigned to the machine tool (2, 2a), is different from the encryption key and is provided for the decryption, and which module enables the machine control parameters for controlling the machine tool (2, 2a) only in the case of successful decryption, with an associated method of avoiding improper machine activation by machine control parameters, and also an associated data carrier or data carrier signal and a method, system and program for generating such parameters.